(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020030021778 A
(43)Date of publication of application: 15.03.2003

(21)Application number: 1020010055190
(22)Date of filing: 07.09.2001

(71)Applicant: ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE

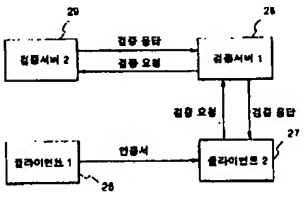
(72)Inventor: CHO, SANG RAE
CHO, YEONG SEOP
CHOI, DAE SEON
JIN, SEUNG HEON
JUNG, GYO IL
KIM, HUI SEON
KIM, TAE SEONG
LEE, JEONG HYEON
NOH, JONG HYEOK

(51)Int. Cl H04L 9/30

(54) METHOD AND APPARATUS OF VERIFYING VALIDITY OF CERTIFICATE OF AUTHENTICATION USING VERIFICATION SERVER AT PUBLIC KEY INFRASTRUCTURE

(57) Abstract:

PURPOSE: A method and apparatus of verifying validity of certificate of authentication using a verification server at a public key infrastructure are provided, which are capable of securing mutual interlocking of a public key infrastructure of different systems and of reducing a load of a client for verification.



CONSTITUTION: The first verification server(28) receives validity verification request of a certificate of authentication from a verification request means(27) and judges whether or not of a reliable domain. The first verification server(28) compares and judges a routing server list to perform the validity verification of the certificate of authentication. The second verification server(29) receives validity verification request of a certificate of authentication from the first verification server and judges whether or not of an access allowance server list. The second verification server(29) performs the validity verification of the certificate of authentication.

Legal Status
Date of request for an examination (20010907)
Final disposal of an application (registration)
Date of final disposal of an application (20040128)
Patent registration number (1004194840000)
Date of registration (20040209)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
H04L 9/30

(11) 공개번호 특2003-0021778
(43) 공개일자 2003년03월15일

(21) 출원번호 10-2001-0055190
(22) 출원일자 2001년09월07일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 조영섭
대전광역시유성구신성동142-11상가주택301호
최대선
대전광역시서구월평동황실타운118-905
진승헌
대전광역시서구월평2동백합아파트104동1405동
조상래
대전광역시유성구송강동청솔아파트512동1408호
이정현
대전광역시유성구송강동청솔아파트512동1408호
김희선
대전광역시유성구가정동236-1구332
김태성
대전광역시유성구송강동200-1한솔아파트203동705호
노종혁
인천광역시남동구구월3동1376-7
정교일
대전광역시유성구신성동한울아파트107동1102호

(74) 대리인 이화익

심사청구 : 있음

(54) 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성검증 장치 및 방법

요약

본 발명은 공개키 기반구조에서 인증서 유효성의 검증에 관한 것으로, 특히 유무선 환경의 공개키 기반구조에서 클라이언트가 수신 받은 인증서의 유효성을 검증서버에 요청하고, 검증서버는 요청 받은 인증서의 도메인을 검사하여 검증서버 에 자신이 속해 있는 도메인일 경우 인증서 검증 작업을 실시하며, 검증서버에 등록되어 있는 외부 도메인일 경우에

는 외부의 도메인을 처리하는 다른 검증서버로 인증작업을 라우팅하므로써 인증서 검증에 대한 클라이언트의 부하를 줄이고 검증서버가 처리하는 도메인뿐만 아니라 외부의 도메인 사이에서 효과적인 연동을 하여 인증서의 유효성을 검증하는 것이다.

본 발명은 공개키 기반구조를 가지는 유무선 인터넷 상에서 인증서의 유효성 여부를 검증서버를 구성하여 처리하고, 신뢰 서버 목록과 라우팅 서버 목록을 설정하여 검증서버가 처리하는 도메인일 경우에는 직접 처리하고 외부 도메인일 경우에는 라우팅하여 해당 신뢰 도메인의 인증서의 유효성 검증을 처리하는 검증서버로 송신하여 신뢰관계가 있는 인증서의 유효성 검증에 상호 연동이 가능하다.

대표도

도 1

색인어
공개키 기반구조, 검증서버, 인증서의 유효성 검증, 클라이언트, 도메인

명세서

도면의 간단한 설명

도 1은 본 발명의 공개키 기반구조에서 인증서의 유효성을 검증하는 장치의 개략도.

도 2는 본 발명에 따른 검증서버1, 2의 구성을 개략적으로 도시한 도면.

도 3은 본 발명의 검증서버 1에서의 인증서의 유효성 검증의 라우팅을 위한 라우팅 서버 목록 및 신뢰 서버 목록 등록의 동작 순서도.

도 4는 본 발명의 검증서버 1에서 클라이언트 2로부터 인증서의 유효성 검증 요청이 입력되었을 때 검증서버 1에서 자체 처리하거나 다른 검증서버 2로 라우팅하는 동작의 순서도.

도 5는 검증서버 2에서 접근허용 도메인 목록을 등록하는 순서도.

도 6은 인증서의 유효성 검증요청을 검증서버 2에서 처리하여 검증서버 1로 송신하는 순서도.

도 7은 검증서버 2로부터 인증서의 유효성의 검증 결과를 수신 받아 검증서버 1에서 처리하여 클라이언트 2로 송신하는 동작 순서도.

< 도면의 주요 부분에 대한 설명>

26, 27 : 클라이언트 1, 2 28, 29 : 검증서버 1, 2

30, 37 : 통신모듈 31 : 검증요청분석모듈

32 : 저장모듈 33 : 비교모듈

34 : 검증처리모듈 35 : 오류처리모듈

36 : 응답생성모듈

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 공개키 기반구조(Public Key Infrastructure)에서 인증서 유효성의 검증에 관한 것으로, 특히 유무선 환경의 공개키 기반구조에서 클라이언트가 수신 받은 인증서의 유효성을 검증서버에 요청하고, 검증서버는 요청받은 인증서의 도메인을 검사하여 검증서버에서 직접 처리하는 도메인일 경우 인증작업을 실시하며, 검증서버에 등록되어 있는 외부의 도메인일 경우에는 외부의 도메인을 처리하는 검증서버로 인증작업을 라우팅하므로써 인증서 검증에 대한 클라이언트의 부하를 줄이고 검증서버가 처리하는 도메인뿐만 아니라 외부의 도메인 사이에서 효과적인 연동을 하여 인증서의 유효성을 검증할 수 있는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 장치 및 방법에 관한 것이다.

공개키 기반 구조는 공개키 암호 방식을 사용하는 암호 시스템에서 사용자의 공개키를 안전하고 신뢰성 있게 공표하여, 사용자가 공개키 인증서를 이용하여 전자상거래에서의 기밀성, 무결성, 인증, 부인봉쇄 기능을 제공 받게 하는 정보보호 기반구조이다.

공개키 기반 구조는 공개키에 대한 인증서를 발급하는 인증기관, 사용자에게 인증서 발급 요청을 등록하고 신원 확인 기능을 수행하는 등록기관, 그리고 인터넷 상의 다양한 사용자와 응용이 인증기관에서 발급한 인증서를 쉽게 검색할 수 있도록 인증서를 저장 관리하는 디렉토리 서버 등으로 구성된다.

현재 공개키 기반 구조를 기반으로 전자상거래의 안전성을 확보하려는 연구가 많이 진행되었고 전자상거래의 정보보호 기반구조로 활용되고 있으며 보다 다양한 응용 서비스를 지원하기 위한 연구가 활발히 진행되고 있다.

한국특허 출원번호 10-2000-0065370 " 이중전자 서명을 사용한 인증 확인 대행 서비스 제공시스템" 은 무선단말기에서 무선단말기 간의 엔드투엔드(end-to-end : EtoE) 메시지 보안과 공개키 기반의 송신자 인증 서비스를 제공하기 위한 것으로, 제한된 용량의 무선단말기에서 수행하기 어려운 인증서 검증작업을 대행해주는 이중 전자 서명을 사용한 인증 확인 대행 서비스 제공 시스템이다. 무선망 환경의 단말기는 제한된 용량을 가지고 있기 때문에 인증서의 유효성 검증 작업을 수행하는 것이 매우 어려운데 이를 대행해주는 기능을 수행한다. 해당 특허의 인증 확인 대행 시스템에서는 메시지 송신자가 보낸 인증서에 대한 인증서 폐기목록 검사 및 유효성 검사를 대행해줌으로써 수신 무선단말기에서는 별도의 인증서 폐기목록 검사 등 송신자 인증서의 유효성 확인 절차 없이 인증서를 바로 사용할 수 있도록 하였다. 무선 단말기를 통해 메시지를 송수신하는 무선망 환경에서 공개키 기반의 인증 보안 서비스를 필요로 하는 모든 응용 서비스 제공에 활용 가능하다.

선행특허는 무선환경만을 대상으로 검증기능을 이관하는 것이며 무선망에서의 시스템 효율이 대상이 된다.

또한, Prandini, M이 IEEE Computer Security Applicaton Conference 에 1999년 15권 1호, PP. 276~281에 발표한 " Efficient certificate status handling within PKIs: an application to public administration services" 에 발표한 선행논문에 따르면 공개키 기반 구조가 정보보호 기반 구조로 활용됨에 따라 인증서의 유효성을 검증하는 것에 많은 관심과 연구가 진행되고 있다. 인증서 유효성 검증 방식의 대표적인 것은 인증서 폐기목록(Certification Revocation List), OCSP(Online Certificate Status Protocol) 이다. 선행논문은 웹 환경에서의 적절한 인증의 상태 검증 방식으로 인증서 폐기목록과 OCSP를 활용한 공개키 기반구조 모델을 제시하고 검증기술을 이용한 시스템의 구성에 관한 것이다.

현재 대부분의 공개키 기반 구조에서는 인증서 유효여부에 대한 검증은 클라이언트가 인증서 폐기목록을 사용하여 수행하고 있다. 인증서 폐기목록은 일정 주기마다 인증기관에서 갱신을 하며, 각 인증기관마다 root 인증서에 대한 하나의 인증서 폐기목록을 유지하며 root 인증서가 폐기될 때까지 인증서 폐기목록은 축적된다. 이로 인해 인증서 폐기목록은 데이터 크기에 대한 오버헤드가 문제가 되고 있고 실시간으로 인증서의 상태 검증은 불가능 하다. 이러한 문제를 해결하기 위하여 CRL DP, Delta CRL, CRT, OCSP 등이 제안되었다.

이러한 인증서 유효 여부 검증 방법 중 크기 문제뿐만 아니라 적시성을 제공하는 방법으로 OCSP가 있다. 현재 IETF PKIX 워킹그룹에서 버전 2가 진행중인 상태이며, 실시간 인증서 검증 서비스인 ORS(Online Revocation Status) 뿐만 아니라 인증 경로 구축을 위한 DPD(Delegated Path Discovery), 인증 경로 검증을 위한 DPV(Delegated Path Validation)를 제공하고 있다.

그러나, 이러한 OCSP는 인증서 검증에 관련된 기반 기술임에는 틀림없지만 실제 적용을 위한 메커니즘을 제시하고 있지 않으며, 클라이언트가 검증하고자 하는 인증서의 도메인이 외부의 도메인일 경우, 외부 도메인에 속한 검증 서버들에게 인증서의 검증을 직접 요청하고 응답을 신뢰해야 한다는 클라이언트의 부담이 문제점이 된다.

발명이 이루고자 하는 기술적 과제

본 발명은 상술한 바와 같은 문제점을 해결하기 위한 것으로, 공개키 기반구조를 가지는 유무선 인터넷 상에서 인증서의 유효성 검증을 검증서버를 구성하여 처리하고, 신뢰 도메인 목록과 라우팅할 도메인 목록을 설정하여 검증서버가 처리하는 도메인일 경우에는 직접 처리하고 외부 도메인일 경우에는 라우팅하여 해당 신뢰 도메인의 유효성 검증을 처리하는 검증서버로 송신하여 신뢰관계가 있는 인증서의 유효성 검증에 상호 연동을 제공하여 클라이언트의 부담을 줄이는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 장치 및 방법을 그 목적으로 한다.

발명의 구성 및 작용

상술한 바와 같은 목적을 달성하기 위한 본 발명은,공개키 기반 구조에 있어서 검증요청 수단으로부터 인증서의 유효성 검증 요청을 수신하면 신뢰도메인 여부를 판단하고, 라우팅서버 목록을 비교 판단하여 인증서의 유효성 검증을 수행하는 검증처리 수단 1과, 검증처리 수단 1로부터 인증서의 유효성 검증 요청을 수신하면 접근허용 서버목록과 비교 판단하여 인증서의 유효성 검증을 수행하는 검증처리수단 2; 를 포함한다.

또한, 본 발명의 신뢰도메인 여부를 판단하는 것은 인증서의 발급을 신뢰도메인에서 하였으면 인증서의 유효성 검증 작업을 검증처리수단 1에서 처리하고, 인증서의 발급을 신뢰도메인에서 하지 않았으면, 라우팅 서버목록과 비교하여 해당하면 인증서의 유효성 검증을 검증처리 수단 2로 요청하는 것을 특징으로 한다.

또한, 본 발명은 접근허용 서버 목록과 비교 판단하는 것은, 검증처리수단 1에서 인증서의 유효성 검증을 요청하면 검증처리 수단 1이 접근허용 서버 목록에 해당하면 인증서의 유효성 검증 작업을 처리하며, 검증처리수단 1이 접근허용 서버 목록에 해당하지 않으면 에러 처리하는 것을 특징으로 한다.

또한, 본 발명은 클라이언트로부터 인증서의 유효성 검증 요청을 수신하는 단계, 검증서버 1에서 인증서의 발급기관이 신뢰도메인 여부를 판단하는 단계, 신뢰도메인이면 인증서의 유효성 검증 작업을 수행후 응답을 클라이언트로 송신하는 단계, 인증서의 발급기관이 신뢰도메인이 아니면, 라우팅 서버 목록과 비교하여 해당하면 검증서버 2로 인증서의 유효성의 검증을 요청하는 단계, 라우팅 서버 목록과 비교하여 해당하지 않는 경우 오류 응답을 클라이언트로 송신하는 단계를 포함한다.

또한, 라우팅 서버 목록과 비교하여 해당하면 검증서버 2로 인증서의 유효성의 검증을 요청하면, 검증서버 2는 검증서버 1이 접근 허용 서버 목록에 해당하면 인증서의 유효성 검증 작업을 수행하여 검증서버 1로 응답을 송신하며, 검증서버 1이 접근허용 서버 목록에 해당하지 않으면 오류응답처리하여 검증서버 1로 송신하는 것을 포함한다.

또한, 검증서버 1로 응답을 송신하면, 검증서버 2가 신뢰 서버 목록에 해당하면 응답을 클라이언트로 송신하는 단계, 검증서버 2가 신뢰서버 목록에 해당하지 않으면 클라이언트로 에러값을 송신하는 것을 특징으로 한다.

또한, 본 발명은 인증서의 유효성을 검증하는 데 있어서, 클라이언트에서 입력되는 인증서의 유효성 검증 요청 결과를 송수신하는 통신모듈과, 통신모듈에서 입력되는 인증서의 유효성 검증 요청을 분석하는 검증요청분석 모듈, 검증요청분석 모듈의 결과와 저장모듈의 정보를 비교 판단하는 비교모듈, 비교모듈의 결과에 따라 검증 요청을 처리하는 검증처리모듈, 요청을 처리한 결과로 응답을 생성하는 응답생성모듈을 포함한다.

이하, 본 발명에 따른 실시 예를 첨부한 도면을 참조하여 상세히 설명하면 다음과 같다.

도 1은 본 발명의 공개키 기반구조에서 인증서의 유효성을 검증하는 장치의 개략도로 설명하면 다음과 같다.

구성은 공개키 기반 구조에서 인증서를 사용하는 클라이언트 1(26)과 클라이언트 2(27), 그리고 인증서의 유효성을 검증해주는 검증서버 1(28)과 검증서버 2(29)로 이루어 진다.

클라이언트 1(26)의 인증서의 도메인은 검증서버 2(29)의 신뢰 도메인이어서 클라이언트 1(26)의 인증서에 대한 유효성을 검증서버 2(29)가 검증할 수 있으며, 클라이언트 2(27)의 인증서의 도메인은 검증서버 1(28)의 신뢰 도메인이어서 클라이언트2(27)의 인증서에 대한 유효성을 검증서버 1(28)이 검증할 수 있다.

한편, 검증서버 1(28)이 인증서의 유효성을 검증할 때, 검증서버 1(28)에서 검증작업을 실시하지 못하는 인증서, 즉 검증서버 1(28)에서 신뢰하는 도메인이 아닌 외부의 도메인인 인증서에 대하여는 검증작업을 수행할 수 있는 다른 검증서버 2(29)로 검증작업을 요청을 한다.

검증서버 1(28)은 다른 검증서버 2(29)로 인증서의 유효성에 대한 검증작업을 요청하기 위해서는 라우팅 서버 목록의 등록, 신뢰 서버 목록의 등록이 필요하며, 검증서버 2(29)에서 검증 요청에 대한 작업의 수행 여부를 판단하기 위해 접근허용 서버의 목록을 등록하는 작업이 요구된다.

클라이언트 2(27)에서 클라이언트 1(26)의 인증서에 대한 유효성을 검증하려면, 클라이언트 2(27)는 검증작업을 처리하는 검증서버 1(28)로 인증서의 유효성 검증 요청 메시지를 송신하고 검증서버 1(28)에서 요청받은 인증서의 도메인을 검사하여 검증서버 1(28)에서 직접 처리하는 도메인일 경우 검증작업을 실시하며, 검증서버 1(28)에 등록되어 외부의 도메인일 경우에는 외부의 도메인를 처리하는 검증서버 2(29)로 검증작업을 라우팅할 수 있어서 검증서버 1(28)에서 처리하는 도메인뿐만 아니라 외부의 도메인도 효과적인 연동을 하여 인증서의 유효성을 검증할 수 있다.

한편, 도 2는 본 발명에 따른 인증서의 유효성 검증작업을 처리하는 검증서버 1, 2(28, 29)의 구성을 개략적으로 도시한 것으로 설명하면 다음과 같다.

구성은 송신과 수신을 담당하는 통신모듈(30, 37)과, 인증서의 유효성의 검증 요청을 분석하는 검증요청분석모듈(31)과 정보를 저장하고 있는 저장모듈(32)에서 데이터를 읽어와서 비교 판단하는 비교모듈(33)과 비교모듈(33)에서 오류 발생 결과를 수신하였을 경우 오류를 처리하는 오류처리모듈(35)과 검증 요청을 처리하는 검증 처리 모듈(34)과 응답을 생성하는 응답생성 모듈(36)과 결과를 클라이언트나 검증서버로 송신하는 통신모듈(37) 등으로 이루어진다.

도 3은 검증서버 1(28)에서의 인증서의 유효성 검증의 라우팅을 위한 라우팅 서버 목록 및 신뢰 서버 목록 등록의 동작 순서도로 설명하면 다음과 같다.

먼저 인증서의 유효성의 검증을 검증서버 1(28)에서 처리하지 못하는 경우 다른 검증 서버 2(29)에게 라우팅할 수 있도록 라우팅 서버 목록을 저장 모듈에 등록한다(스템 S40, S41).

다음 단계로 검증서버 1(28)은 신뢰 서버 목록을 작성하여 저장모듈(32)에 저장을 한다(스텝 S42, S43).

도 4는 본 발명의 검증서버 1(28)에서 클라이언트 2(27)로부터 인증서의 유효성 검증 요청이 입력되었을 때 검증서버 1(28)에서 자체 처리하거나 다른 검증서버 2(29)로 라우팅하는 동작의 순서도로 설명하면 다음과 같다.

클라이언트 2(27)로부터 인증서의 유효성을 검증하는 요청이 수신되면 검증요청분석모듈(31)에서는 검증이 요청된 인증서의 도메인을 파악하고 검증서버 1(28)에서 직접 처리할 수 있는 도메인인지 여부를 판단한다(스텝 S50, S51, S52).

클라이언트 2(27)가 검증을 요청한 인증서의 도메인이 검증서버 1(28)에서 신뢰하는 도메인과 일치할 경우에는 클라이언트 2(27)에서 송신한 인증서의 유효성을 검증작업을 수행하고 검증 응답 메시지를 생성한 후 통신모듈(30. 37)에서 클라이언트 2(27)에게 검증 응답 메시지을 전달한다(스텝S53, S54, S55).

한편, 클라이언트 2(27)가 검증을 요청한 인증서의 도메인이 검증서버 1(28)에서 신뢰하는 도메인과 일치하지 않을 경우에는 다른 검증서버 2(29)에서 처리할 수 있는 인증서인지를 판단하기 위해 저장모듈(32)에 기저장된 라우팅 서버 목록을 읽어와서 라우팅 서버 목록과 검증 요청 대상인 인증서의 도메인을 비교하여, 라우팅 서버 목록과 일치하지 않는 경우에는 오류처리모듈(35)에서 응답 생성 모듈(36)로 에러를 출력하여 클라이언트 2(27)에 전달한다(S56, S57, S60).

클라이언트 2(27)가 요청한 인증서의 도메인이 라우팅 서버 목록과 일치할 경우에는 다른 검증서버 2(29)로 인증서의 유효성 검증을 요청한다(스텝 S58, S59).

도 5는 검증서버 2(29)에서 다른 검증서버 1(28)로부터 인증서 검증 요청을 받았을 시에 검증 요청에 대한 작업을 수행할 것인지 거부할 것인지를 판단하기 위한 접근 허용 서버 목록을 저장하는 순서도이다.

검증서버 2(29)에서는 다른 검증서버 1(28)로부터 인증서 검증 요청을 수신시에 인증서의 유효성 검증작업을 실시할 것인지 거부할 것인지 선택하는데 사용하기 위해 접근허용 서버 목록을 기록 저장하며, 검증 요청시에 저장된 접근허용 서버 목록을 검색하여 인증서의 검증작업을 수행 또는 거부하는 것이다(스텝 S61, S62).

도 6은 검증서버 1(28)에서 요청한 인증서의 유효성 검증요청을 검증서버 2(29)에서 처리하여 결과를 검증서버 1(28)로 송신하는 순서도로 설명하면 다음과 같다.

검증서버 2(29)의 통신모듈(30)에서 검증서버 1(28)이 요청한 인증서의 유효성 검증 처리 요청을 송신하면 검증요청분석모듈(31)에서는 검증 요청에 대한 작업을 수행할 것인지 거부할 것인지를 판단하기 위해 저장모듈(32)에 저장된 접근허용 서버 목록을 읽어온다(스텝 S70, S71, S72).

인증서의 유효성 검증을 요청한 검증서버 1(28)과 접근허용 서버 목록을 비교하여 일치하지 않을 경우에는 오류처리모듈(35)에서 오류 처리를 하고 요청을 수행하지 않았다는 응답을 생성하고 통신모듈(30)에서 검증서버 1(28)로 전송한다(S73, S75, S76, S77).

한편, 인증서의 유효성 검증을 요청한 검증서버 1(28)과 접근허용 서버 목록을 비교하여 일치하면 인증서의 유효성 검증처리모듈(34)에서 유효성을 검증하고 응답생성 모듈(36)에서 응답 메시지를 생성한 후 통신모듈(37)을 통하여 검증서버 1(28)로 송신한다(S73, S74, S75, S77).

도 7은 검증서버 2(29)로부터 인증서의 유효성의 검증 결과를 수신 받아 검증서버 1(28)에서 처리하여 클라이언트 2(27)로 송신하는 동작 순서도로 설명하면 다음과 같다.

검증서버 2(29)로부터 인증서의 유효성의 검증 결과를 수신하면 검증 응답을 분석한 후 저장모듈(32)에 저장되어 있는 신뢰 서버 목록을 획득하여 검증을 응답한 검증응답 서버와 비교하여 일치하지 않을 경우에는 오류처리모듈(35)에서 오류 처리를 하고 응답 생성 모듈(36)에서 요청을 수행하지 못했다는 응답을 생성하고 통신모듈(37)에서 클라이언트 2(27)로 송신한다(스텝 S80, S81, S82, S83, S85, S86).

한편, 검증을 응답한 검증응답 서버와 신뢰 서버 목록이 일치할 경우에는 응답생성모듈(36)에서 결과값을 통신모듈(37)로 전송하여 클라이언트 2(27)로 송신한다(S84, S86).

이상과 같이, 본 발명은 공개키 기반구조에서 검증서버를 이용하여 인증서의 유효성을 검증하는 것에 관한 것으로, 클라이언트에서 인증서의 유효성 검증을 검증서버에 요청하고, 검증서버는 검증 요청 대상인 인증서의 도메인을 검사하여 검증서버에서 직접 처리하는 도메인일 경우 인증작업을 실시하며, 검증서버에서 등록되어 있는 외부의 도메인일 경우에는 외부의 도메인을 처리하는 검증서버로 인증작업을 라우팅 함으로써 인증서 검증에 대한 클라이언트의 부하를 줄이고 검증서버가 처리하는 도메인 뿐만 아니라 외부의 도메인 사이에서 효과적인 연동을 하여 인증서의 유효성을 검증할 수 있다.

발명의 효과

이상과 같이, 본 발명은 공개키 기반 구조에서 상호연동을 위한 검증서버 간의 신뢰관계 관리 방법은 인증서 유효성 검증을 서버가 수행하고 검증서버 간의 신뢰관계 관리를 집중된 통제하에 수행하여 줌으로써 검증에 대한 클라이언트의 부담을 줄이면서 신뢰 도메인이 다른 여러 체계의 공개키 기반 구조의 상호 연동성을 보장해 줄 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

공개키 기반 구조에 있어서.

검증요청 수단으로부터 인증서의 유효성 검증 요청을 수신하면 신뢰도메인 여부를 판단하고, 라우팅서버 목록을 비교 판단하여 상기 인증서의 유효성 검증을 수행하는 제 1 검증서버;

상기 제 1 검증서버로부터 상기 인증서의 유효성 검증 요청을 수신하면 접근허용 서버목록과 비교 판단하여 상기 인증서의 유효성 검증을 수행하는 제 2 검증서버; 를 포함하는 것을 특징으로 하는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 장치.

청구항 2.

제 1항에 있어서, 상기 제 1 검증서버는,

상기 신뢰도메인 여부를 판단 결과, 상기 인증서의 발급이 신뢰도메인에서 이루어진 경우 상기 인증서의 유효성 검증 작업을 처리하고,

상기 인증서의 발급이 신뢰도메인에서 이루어지지 않았을 경우, 상기 라우팅 서버 목록과 비교하여 해당하면 상기 인증서의 유효성 검증을 상기 제 2 검증서버로 요청하는 것을 특징으로 하는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 장치.

청구항 3.

제 1항에 있어서, 상기 제 2 검증서버는,

상기 제 1 검증서버에서 인증서의 유효성 검증을 요청하면 상기 제 1 검증서버가 접근허용 서버 목록에 해당하면 상기 인증서의 유효성 검증 작업을 처리하며,

상기 제 1 검증서버가 접근허용 서버 목록에 해당하지 않으면 상기 제 1 검증서버로 에러를 송신하는 것을 특징으로 하는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 장치.

청구항 4.

제 1항에 있어서, 상기 제 1 검증서버는,

클라이언트에서 입력되는 인증서의 유효성 검증 요청 결과를 송수신하는 통신모듈과;

상기 통신모듈에서 입력되는 인증서의 유효성 검증 요청을 분석하는 검증요청분석 모듈과;

상기 검증요청분석 모듈의 결과와 저장모듈의 정보를 비교 판단하는 비교모듈과;

상기 비교모듈의 결과에 따라 검증 요청을 처리하는 검증처리모듈과,

상기 요청을 처리한 결과로 응답을 생성하는 응답생성모듈을 포함하는 것을 특징으로 하는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 장치.

청구항 5.

제 1항에 있어서, 상기 제 2 검증서버는,

상기 제 1검증서버에서 입력되는 인증서의 유효성 검증 요청 결과를 송수신하는 통신모듈과;

상기 통신모듈에서 입력되는 인증서의 유효성 검증 요청을 분석하는 검증요청분석 모듈과;

상기 검증요청분석 모듈의 결과와 저장모듈의 정보를 비교 판단하는 비교모듈과;

상기 비교모듈의 결과에 따라 검증 요청을 처리하는 검증처리모듈과,

상기 요청을 처리한 결과로 응답을 생성하는 응답생성모듈을 포함하는 것을 특징으로 하는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 장치.

청구항 6.

클라이언트로부터 인증서의 유효성 검증 요청을 수신하는 단계와;

검증서버 1에서 상기 인증서의 발급기관이 신뢰도메인 여부를 판단하는 단계;

신뢰도메인이면 인증서의 유효성 검증 작업을 수행후 응답을 클라이언트로 송신하는 단계;

상기 인증서의 발급기관이 신뢰도메인이 아니면, 라우팅 서버 목록과 비교하여 해당하면 검증서버 2로 상기 인증서의 유효성 검증을 요청하는 단계;

상기 검증서버 2는 상기 검증서버 1을 상기 라우팅 서버 목록과 비교하여 해당하지 않는 경우 오류 응답을 상기 검증서버 1로 송신하는 단계를 포함하는 것을 특징으로 하는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 방법.

청구항 7.

제 6항에 있어서, 상기 인증서의 유효성 검증을 요청하는 단계는,

상기 검증서버 2는 상기 검증서버 1이 접근 허용 서버 목록에 해당하면 상기 인증서의 유효성 검증 작업을 수행하여 상기 검증서버 1로 응답을 송신하며,

상기 검증서버 1이 상기 접근허용 서버 목록에 해당하지 않으면 오류처리하여 오류응답을 검증서버 1로 송신하는 것을 특징으로 하는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 방법.

청구항 8.

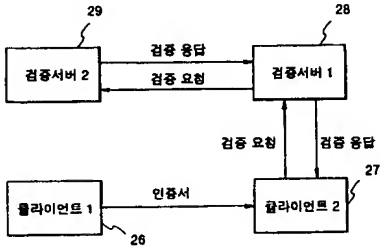
제 7항에 있어서, 상기 인증서의 유효성 검증 작업을 수행하여 상기 검증서버 1로 응답을 송신하면,

상기 검증서버 2가 신뢰 서버 목록에 해당하면 상기 응답을 클라이언트로 송신하고;

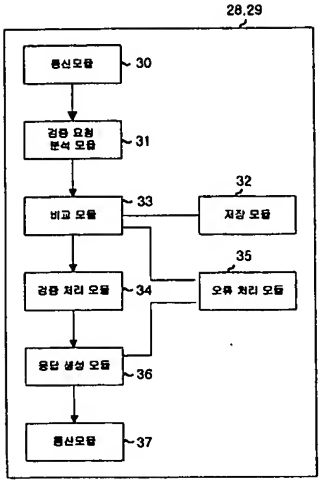
상기 검증서버 2가 신뢰서버 목록에 해당하지 않으면 상기 클라이언트로 에러값을 송신하는 것을 특징으로 하는 공개키 기반구조에서 검증서버를 이용한 인증서의 유효성 검증 방법.

도면

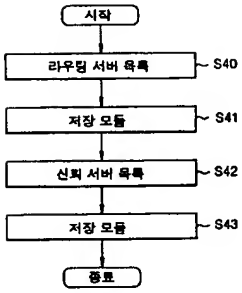
도면 1



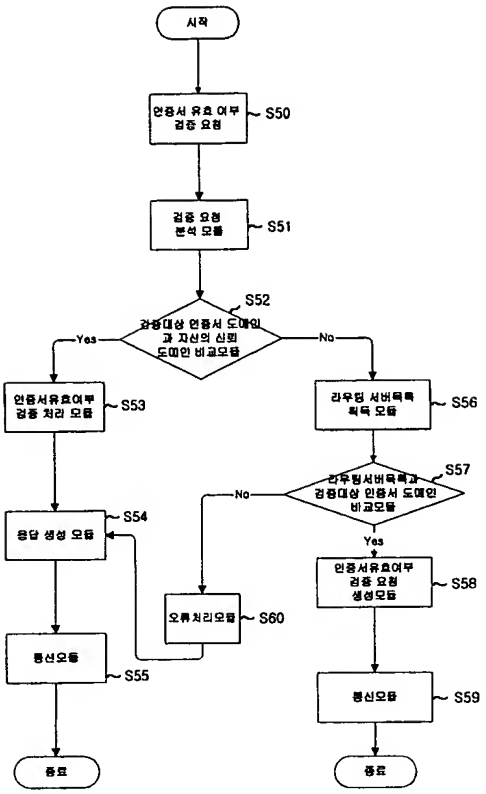
도면 2


28,29
통신모듈
30
검증 요청 분석 모듈
31
32
비교 모듈
33
저장 모듈
35
검증 처리 모듈
34
오류 처리 모듈
응답 생성 모듈
36
통신모듈
37

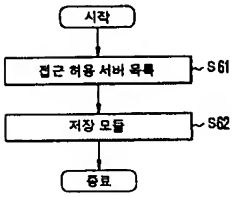
도면 3


시작
라우팅 서버 등록
S40
저장 모듈
S41
신뢰 서버 등록
S42
저장 모듈
S43
종료

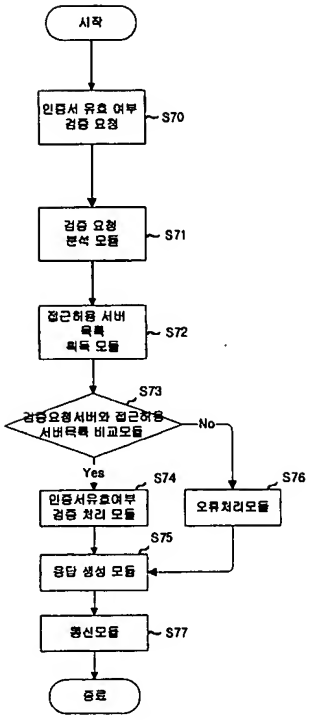
도면 4


시작
인증서 유효 여부 검증 요청
S50
검증 요청 분석 모듈
S51
S52
검증대상 인증서 도메인과 자신의 신뢰 도메인 비교모듈
Yes
No
인증서유효여부 검증 처리 모듈
S53
라우팅 서버목록 획득 모듈
S56
S57
라우팅서버목록과 검증대상 인증서 도메인 비교모듈
No
Yes
응답 생성 모듈
S54
오류처리모듈
S60
인증서유효여부 검증 요청 생성모듈
S58
통신모듈
S55
통신모듈
S59
종료
종료

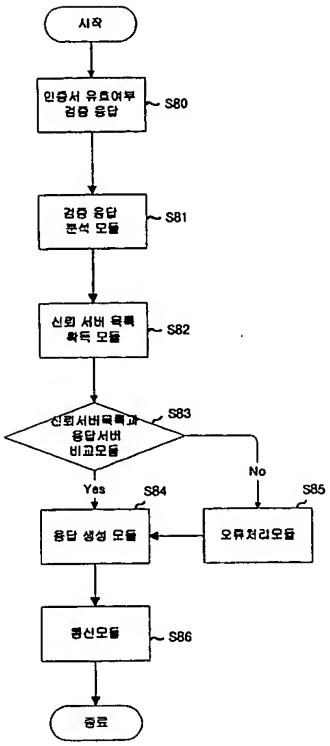
도면 5


시작
접근 허용 서버 목록
S61
저장 모듈
S62
종료

도면 6


시작
인증서 유효 여부 검증 요청
S70
검증 요청 분석 모듈
S71
접근허용 서버 목록 획득 모듈
S72
S73
검증요청서버와 접근허용 서버목록 비교모듈
No
Yes
인증서유효여부 검증 처리 모듈
S74
오류처리모듈
S76
응답 생성 모듈
S75
통신모듈
S77
종료

도면 7


시작
인증서 유효여부 검증 응답
S80
검증 응답 분석 모듈
S81
신뢰 서버 목록 확득 모듈
S82
신뢰서버목록과 응답서버 비교모듈
S83
Yes
No
S84
S85
응답 생성 모듈
오류처리모듈
통신모듈
S86
종료